centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC 1506

## Procedimiento de Empleo Seguro
## *EP880*

Noviembre 2021

MINISTERIO DE DEFENSA

**Catálogo de Publicaciones de la Administración General del Estado**
**https://cpage.mpr.gob.es**

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.01.28 10:40:22 +01'00'


NIPO: 083-21-230-X.

Fecha de Edición: Noviembre de 2021.

# ÍNDICE

# 1. INTRODUCCIÓN

## 1.1 PROPÓSITO

1. Este documento contiene el procedimiento de empleo seguro del *software* de **cifrado off-line EP880** de EPICOM y su material asociado, cuando se utilice para proteger el almacenamiento de información en sistemas bajo el alcance del ENS.
2. Todas las configuraciones de seguridad recogidas en este procedimiento de empleo seguro deben ser aplicadas para disponer de la versión del producto que ha sido cualificada e incluida en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC).

## 1.2 APLICABILIDAD

3. Este documento es aplicable a la partir de la versión **2.08.36** del EP880.
4. Este procedimiento aplica a todos los usuarios del *software* y, por tanto, debe ser tenido en cuenta por todas las organizaciones que vayan a hacer uso del producto en sistemas bajo el alcance del ENS.

## 2. DESCRIPCIÓN DEL CRIPTOSISTEMA

5. El EP880 es una aplicación de cifrado *off-line* que se ejecuta en un ordenador con sistema operativo Windows y que permite proteger archivos, tanto en el disco duro como en dispositivos de almacenamiento externo conectados al ordenador en el que la aplicación se está ejecutando para su posterior almacenamiento y/o envío, asegurando su confidencialidad e integridad mediante los siguientes servicios de seguridad:

    a. Cifrar/descifrar archivos (tanto almacenados en el disco duro como en dispositivos de almacenamiento externo conectados al ordenador en el que la aplicación se está ejecutando).

    b. Firmar/verificar digitalmente archivos (tanto almacenados en el disco duro como en dispositivos de almacenamiento externo conectados al ordenador en el que la aplicación se está ejecutando).

6. La aplicación también ofrece la posibilidad de integración con el cliente de correo Microsoft Outlook 2013.

### 2.1 COMPONENTES DEL SISTEMA

7. Los componentes básicos del software de cifrado *off-line* EP880 se reducen a una **aplicación *software*** que, una vez instalada en el equipo, cifrará o descifrará la información bajo demanda del usuario.

### 2.2 ESTADOS OPERACIONALES DEL *SOFTWARE* DE CIFRADO

8. Los posibles estados de EP880 son:

    a. **APAGADO / CERRADO:** El *software* estará cerrado y no será posible hacer uso de sus funcionalidades de cifrado o descifrado.

        i. No es posible acceder a la información cifrada con el EP880.

        ii. Todos los parámetros críticos de seguridad (claves y certificados) con los que se cifran los archivos están protegidos.

    b. **AUTENTICADO:** El *software* está encendido / abierto y la autenticación se ha realizado correctamente. Cuando el dispositivo se encuentra en este modo:

        i. Es posible acceder a la información cifrada con el EP880 (siempre que se dispongan las claves correspondientes).

        ii. Las claves de cifrado se encuentran cargadas en memoria volátil del equipo.

## 2.3 PERFILES DE OPERACIÓN Y ADMINISTRACIÓN

9. Solo se define un único perfil de usuario:

    a. **Usuario:** Se habilita después de superar la autenticación del usuario estándar con éxito. Permite acceder a información cifrada siempre y cuando se disponga de las claves correspondientes.

# 3. GESTIÓN

## 3.1 ENTREGA SEGURA DEL PRODUCTO

10. La aplicación EP880 es un producto de *software* desarrollado por **EPICOM S.A**. que se distribuye directamente a los usuarios finales o a través de un administrador de su organización que disponga de la herramienta de servidor de licencias de la aplicación.
11. Por lo tanto, el usuario que quiera utilizar esta aplicación debe primero identificar si tiene en su organización a un administrador de licencias del EP880 y ponerse en contacto con él o bien contactar directamente con EPICOM (ep880.smanto@epicom.es) para que le proporcione una licencia.
12. Cuando un usuario final adquiere la aplicación EP880 deberá iniciar un proceso de dos (2) fases:
    a. Una primera en la que, o bien EPICOM o bien el administrador de licencias del EP880 de su organización, al que se le denominará interlocutor, le entregará el siguiente material:
        i. Dos (2) ficheros de instalación .exe para los distintos sistemas operativos de Windows:
            1. Para *Windows 7, 8.x, 10* de *32 bits (EP880_Setup_32.exe).*
            2. Para *Windows 7, 8.x, 10, Server 2008 R2* de *64 bits (EP880_Setup_64.exe).*
        ii. Manual de Usuario del EP880 (*EP270E880ZZ01*)
    b. Cuando el usuario proceda a instalar la aplicación en el ordenador que haya elegido, el programa le pedirá una serie de datos y generará un fichero de solicitud de licencia. Estos datos y la solicitud de licencia se los deberá trasladar a su interlocutor para que le genere el fichero de licencia.
    c. Comienza entonces la segunda fase en la que el usuario final recibirá un fichero de licencia de su interlocutor con el que podrá finalizar la instalación. Este fichero se corresponderá con una licencia que estará asociada al ordenador donde se instaló el EP880 y no podrá funcionar en otro distinto.
    d. El usuario final debe comprobar:
        i. Que el interlocutor que le entrega el material de instalación del EP880 es confiable, es decir, que es un representante autorizado de la empresa EPICOM o es el administrador de licencias de su organización.
        ii. Que la versión instalada se corresponde con la que le ha indicado su interlocutor.
        iii. Que la aplicación se instala correctamente y se ejecuta también correctamente una vez licenciada.

## 3.2 CONSIDERACIONES PREVIAS

13. La licencia de la aplicación EP880 va ligada a la dirección MAC de la primera interfaz de red habilitada detectada al crear el fichero de solicitud de licencia, por lo que es necesario que esta interfaz esté habilitada en el momento de la verificación de la licencia del EP880.
14. Previamente a la instalación de la aplicación EP880 es necesario cambiar la configuración de *Control de cuentas de usuario* de Windows, utilizando un usuario de Windows y seleccionando el nivel *Predeterminado* para la recepción de notificaciones acerca de cambios en el equipo.

## 3.3 INSTALACIÓN DEL SOFTWARE DE CIFRADO OFFLINE EP880

15. El EP880 debe instalarse en un PC que debe cumplir con los siguientes requisitos hardware y software mínimos:
    a. Requisitos *hardware*:
        i. Procesador a 1 GHz.
        ii. 1 GB de RAM (32-bits) o 2GB de RAM (64-bits).
        iii. Tarjeta gráfica *DirectX* 9 con controlador *WDDM* 1.0 o Superior.
        iv. 50 MB de espacio mínimo disponible en disco duro.
    b. Requisitos *software* (Sistema Operativo *Microsoft Windows* compatible):
        *i. Windows 8.x Profesional 32/64-bit.*
        *ii. Windows 10 Profesional 32/64-bit.*
        *iii. Windows Server 2008 R2.*
16. La resolución de la pantalla y escala (o tamaño de texto) del PC en el que se instala la aplicación, se debe elegir entre cualquiera de las siguientes combinaciones de resoluciones y escalado, para visualizar correctamente las ventanas de la aplicación:
    a. 1920x1080 escala 100 % (Resolución Recomendada)
    b. 1920x1080 escala 125%, escala 150% y escala 175%.
    c. 1680 x 1050 escala 100%, escala 125%, escala 150% y escala 175%.
    d. 1600 x 900 escala 100% y escala 125%.
    e. 1366 x 768 escala 100% y escala 125%.
    f. 1280 x 1024 escala 100%, escala 125% y escala 150%.
    g. 1280 x 720 escala 100%.
    h. 1024 x 768 escala 100% y escala 125%.
    i. 800x600 escala 100%.

17. Para instalar la aplicación EP880 en un ordenador con sistema operativo Windows es necesario utilizar el programa instalador que, o bien EPICOM o bien el administrador de licencias del EP880 de su organización, le haya entregado.
18. A continuación se detallan las instrucciones de instalación de la aplicación EP880 (estas instrucciones se incluyen en el documento REF.1):
    a. Seleccionar el fichero adecuado al ordenador donde se vaya a instalar el EP880 entre los instaladores recibidos (*EP880_Setup_32.exe* o *EP880_Setup_64.exe*).
    b. Ejecutar el fichero de instalación, y seguir los pasos indicados en el instalador seleccionando:
        i. Un directorio de instalación en el que un usuario administrador de Windows tenga permisos de escritura y el usuario de Windows que desee hacer uso del EP880 tenga permisos de lectura y ejecución.
        ii. Los componentes de la aplicación que se deseen instalar. Los componentes de la aplicación son:
            1. *Shell Extension*: permite interactuar con la aplicación desde la interfaz gráfica de Windows.
            2. *Outlook* (a elegir entre la versión para 32bits o 64 bits): permite interactuar con la aplicación desde el cliente de correo de *Microsoft Outlook.*
            3. *Windows Service*: permite interactuar con la aplicación desde línea de comandos. Este componente no forma parte de este procedimiento de empleo.
19. Una vez finalizado el proceso de instalación, es necesario habilitar la funcionalidad del EP880, para lo que se necesita un fichero de licencia válido (tal como se indica en el apartado 3.1 del presente documento).

## 3.4 ACTUALIZACIONES

20. El EP880 es una aplicación SW por lo que para su actualización será necesario un instalador de la nueva versión de la aplicación firmado digitalmente.
21. Una vez recibido el instalador se deberá desinstalar la versión instalada en el PC e instalar la nueva versión.
22. La licencia generada asociada al EP880 de un usuario tiene un periodo de validez ilimitado, siempre y cuando no se modifique ningún aspecto relacionado con el archivo de licencia, como una modificación del lugar donde está almacenada, ni que el ordenador donde se realice la instalación del SW sufra modificaciones que afecten al usuario, como un formateo del PC o una reinstalación del S.O. En estos casos, deberá generarse una nueva petición de licencia para poder volver a utilizar el SW de cifrado offline EP880.

# 4. SEGURIDAD

## 4.1 MODO DE OPERACIÓN SEGURO

23. El EP880 opera por defecto en modo "FIPS-CC" y no requiere ninguna configuración específica por parte del usuario.

## 4.2 AUTENTICACIÓN

24. La licencia generada está vinculada al ordenador en el que se instale el *software* EP880 a través del identificador de la CPU, de la MAC y del usuario del PC. De esta forma, la gestión de usuarios se realiza a través del control de usuarios de Windows, existiendo un único tipo de perfil en el dispositivo, que se utiliza tanto para operación como para administración. El PC donde se está instalado el EP880 debe tener configurado el control de usuarios de Windows, mediante usuario y contraseña.

## 4.3 ADMINISTRACIÓN DEL PRODUCTO

### 4.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

25. La administración se realiza en local a través de la interfaz gráfica mostrada al ejecutar la aplicación EP880 desde el PC en el que se instaló, es decir sólo se permite la gestión local, realizada por usuarios con acceso físico al PC en el que el EP880 está instalado.

### 4.3.2 CONFIGURACIÓN DE ADMINISTRADORES

26. El producto no permite ningún rol de usuario de administración.

## 4.4 SINCRONIZACIÓN HORARIA

27. El PC en el que se instala el EP880 debe mantener la fecha y hora correcta.

## 4.5 AUTO-CHEQUEOS

28. El EP880 realiza los siguientes autochequeos (*self-test*) de integridad del *software* y de la operación de los algoritmos y funciones criptográficas:

    a. ***Power-up self-tests***: Realizados cuando se abre la aplicación desde el ejecutable ubicado en la carpeta de instalación o al invocar las operaciones criptográficas desde el *plugin* de Outlook o desde la *Shell Extension* de *Windows*.

    b. ***Conditional self-tests***.

    c. ***On demand self-test***.

29. El EP880 realiza los siguientes *Power-up self-tests*:
    a. Comprobación de integridad. Verifica que el código del ejecutable y las librerías utilizadas por el sistema no se han modificado. En caso de fallo de este test la aplicación no se ejecutará.
    b. Se comprueba si existe un *debugger* activo. En caso de fallo de este test la aplicación deja de funcionar.
    c. Se realiza una verificación de licencia. En caso de fallo de este test la aplicación no se ejecutará.
    d. Cada vez que el módulo criptográfico se inicia, se llevan a cabo los correspondientes *tests* de los algoritmos criptográficos usados por el EP880, para comprobar que operarán correctamente. Un fallo en cualquiera de estos test impedirá la utilización de la aplicación.
    e. *RNG self-test*: La implementación del generador de números aleatorios lleva a cabo los siguientes *self-tests* para asegurarse de que el DRBG continúa operando como fue diseñado e implementado. Un fallo impedirá la utilización de la aplicación.
    f. Se comprobará la fecha y hora que tiene almacenada el EP880 con la del sistema. Si ésta es anterior, se mostrará un error y se deberá confirmar si se desea continuar utilizando la aplicación en caso de que la diferencia sea menor a 48 horas. En caso contrario, la aplicación no se ejecutará. Si la fecha es posterior, se actualizará la base de datos con la nueva fecha y hora.
    g. Se comprobará la validez de las claves almacenadas en la base de datos y serán invalidadas aquellas que hayan superado la fecha y hora del sistema. Las claves invalidadas no podrán volver a cambiar su estado.
30. El EP880 realiza *Conditional self-tests*. Un fallo en estos test implica que el procedimiento que se está llevando a cabo deje de realizarse.
31. El EP880 realiza los siguientes *on demand self-tests*:
    a. El usuario puede realizar un test de integridad en cualquier instante desde el Interfaz de Usuario, verificando que el código del ejecutable y las librerías utilizadas por el sistema no se han modificado. En caso de fallo de este test la aplicación deja de funcionar.

## 4.6 AUDITORÍA

### 4.6.1 REGISTRO DE EVENTOS

32. La aplicación EP880 implementa una función de gestión de eventos de auditoría del sistema, registrando todas las acciones que se llevan a cabo desde la aplicación. Se almacenan dos (2) tipos de eventos en el sistema: eventos de seguridad y eventos de operación (acciones ejecutadas por el usuario, desde la interfaz gráfica o a través del servicio, tales como gestión de claves o gestión de archivos). Asimismo, en estos archivos de eventos no se almacena ningún

parámetro crítico de seguridad, como puede ser la clave privada o la contraseña asociada a la misma.

33. El EP880 dispone de un menú en su interfaz gráfico para poder visualizar todos los eventos que se producen cuando se realiza alguna acción, adicionalmente los eventos pueden exportarse a un fichero con extensión ".log".

34. Para cada evento registrado en el sistema, se muestran los siguientes campos:

    a. Fecha: día y la hora en la que se registró el evento, mostrando hora, minuto, segundo y milisegundo.

    b. Nivel de criticidad del evento (*info*, *warning*, *error* o *critical*). El campo correspondiente al nivel de criticidad se representa con números en el fichero exportado y corresponde al tercer campo del log, siendo:

        i. 2: *Info*

        ii. 3: *Warning*

        iii. 4: *Error*

        iv. 5: *Critical*

    c. Acción que genera el evento.

    d. Breve descripción del evento.

    e. Tipo de evento (operación o seguridad). Este campo se representa con números en el fichero exportado y se corresponde con el último campo del log, siendo:

        i. 0: Operación

        ii. 1: Seguridad

35. El EP880 ofrece la posibilidad de modificar el tamaño de los dos ficheros de eventos (operación y seguridad) a través de su interfaz gráfica.

### 4.6.2 ALMACENAMIENTO LOCAL

*36.* El EP880 almacena los registros de auditoría de forma local en la BBDD del sistema, que se almacena en el PC donde está instalado el EP880, cuya ruta *C:\Users\Usuario1\AppData\Roaming\EP880\database.*

37. Adicionalmente, es posible configurar la acción a llevar a cabo cuando se complete el tamaño máximo de cada uno de los ficheros de *logs* (operación y seguridad), pudiendo elegir entre rotar el fichero actual, de manera que los nuevos eventos irán sustituyendo a los más antiguos, o crear un nuevo fichero.

    a. Si se elige "*Nuevo fichero*", cuando se complete el tamaño máximo del fichero actual, este fichero (con extensión ".log") será exportado de forma automática a la ruta C:\Users\Usuario[1]\AppData\Roaming\EP880\database.

[1] Usuario debe ser sustituido por el Usuario que esté en uso en el PC donde se instaló el EP880.

El nombre del fichero exportado, comenzará con un código de tres letras que indicará el tipo de logs almacenados en el mismo (OPE: Operacional ó SEG: Seguridad) e incluirá la fecha/hora de la exportación (MM-DD-AA_HH-MM-SS).

## 4.7 *BACKUP*

38. El EP880 genera un *backup* de la base de datos (*Database.db.bck*), almacenándolo en la ruta *C:\Users\Usuario1\AppData\Roaming\EP880\tmp*, cada vez que se produce uno de las siguientes eventos:
    a. Importar un certificado (clave pública) o clave privada
    b. Revocar/eliminar una clave pública o privada
    c. Exportar manualmente eventos a fichero
    d. Crear un nuevo certificado
    e. Vencimiento del periodo de validez de alguna clave.
39. Para restaurar el *backup* realizado de forma automática por el EP880 (*Database.db.bck*), se deberá sustituir el fichero "*Database.db*" ubicado en *C:\Users\Usuario1\AppData\Roaming\EP880\database*, por el fichero de *backup "Database.db.bck*" eliminando la extensión *".bck*".
40. Adicionalmente, el EP880 permite exportar e importar claves tanto públicas (vía fichero "*.pri*", si se trata de una única clave, o "*.lpk*", si se trata de una lista de claves) como privadas (vía fichero "*.der*", si se trata de una única clave, o "*.pub*", si se trata de una lista de claves), para facilitar la distribución y carga de claves. La exportación/importación de claves privadas se utilizará como mecanismo de restauración de las claves tras haber realizado una copia de seguridad de las mismas (con la exportación), realizándose la importación de dichas claves a la base de datos local.

## 4.8 FASE DE OPERACIÓN

41. Durante la fase de operación y mantenimiento del EP880 se se deben tener en cuenta los siguientes aspectos operativos:
    a. Para asegurar la gestión de claves adecuada, comprobar periódicamente que el PC donde está instalado el EP880 se mantiene con la fecha y hora correcta.
    b. La contraseña asociada a la clave privada debe tener una longitud entre 14 y 30 caracteres alfanuméricos, incluyendo al menos una mayúscula, una minúscula, un número y un carácter especial.
    c. La contraseña asociada a la clave privada, debe ser recordada o almacenada en un sitio seguro, ya que el EP880 solicitará la contraseña asociada a la clave privada para realizar las operaciones criptográficas en las que intervenga la clave privada.

d. Debe generarse al menos un par de claves pública-privada.

e. Las contraseñas asociadas a las claves privadas generadas no deben ser almacenadas junto al EP880.

f. Las claves no válidas se deben borrar como máximo a las 2 semanas de se haya superado su periodo de vigencia. Se permite un periodo de gracia en aquellos sistemas cuya distribución retrase la recepción por parte de los destinatarios.

g. Las claves revocadas deberán almacenarse dentro del equipo durante al menos un periodo igual a la vigencia de la misma.

h. En caso de recibir un archivo con un fichero cifrado con una clave revocada, la aplicación advertirá al usuario, el cual debe informar inmediatamente al remitente del archivo y a su cuenta cripto que ha recibido un archivo cifrado con una clave revocada. En caso de que el remitente desconozca el envío este hecho deberá tratarse como un incidente de seguridad.

i. No se deben descifrar archivos cifrados con claves revocadas.

j. Las claves públicas y privadas tendrán un cripto-periodo máximo de 3 meses.

k. Cualquier desviación extendiendo los cripto-periodos de los valores aquí especificados deberá realizarse en base a necesidades operacionales, documentarse y autorizarse por parte de su Responsable de su Seguridad.

l. Para distribuir de manera segura las claves públicas, primero se deberán exportar estas claves, siguiendo las instrucciones del manual de usuario **REF.1**. El archivo ("*.der*", si se trata de una única clave, o "*.pub*", si se trata de una lista de claves) y después se deberán distribuir solo a los destinatarios objetivos, preferiblemente utilizando un método de transporte nominal.

m. Después de abrir la aplicación EP880, esta no debe dejarse desatendida y debe cerrarse inmediatamente tras finalizar su uso.

n. La actualización de la aplicación solo debe ser realizada por un usuario previamente autorizado y siempre que EPICOM o el administrador de licencias del EP880 de su organización, le envíe una nueva versión del producto.

o. La actualización de la aplicación puede afectar a la compatibilidad con versiones anteriores, por lo que en caso de duda deberá consultarse con EPICOM.

p. La validez de la licencia del EP880 es ilimitada, en caso de necesitar una nueva licencia debido a la modificación de alguno de los aspectos del PC/usuario vinculados a la licencia, será necesario realizar una nueva petición de licencia al fabricante.

q. Si la aplicación se encuentra en estado instalada y licenciada, el PC en el que está instalada debe ser almacenado de forma segura o ser custodiado permanentemente por el usuario.

r. Como norma general, si se compromete o pierde material cripto, el usuario lo debe notificar lo antes posible al responsable de su Responsable de su Seguridad y enviar un informe de incidente. Todo el material cripto debe ser revocado y se debe notificar a la Autoridad Operacional para que realice una evaluación del daño.

42. La aplicación EP880 registra de forma automática todas las actuaciones realizadas con el control de eventos, y la integridad tanto de la aplicación como de las operaciones criptográficas realizadas con la misma.

## 4.9 CHECKLIST

| ACCIONES | SÍ | NO | OBSERVACIONES |
|---|---|---|---|
| **DESPLIEGUE E INSTALACIÓN** | | | |
| Verificación de la entrega segura del producto | ☐ | ☐ | |
| Instalación en un entorno seguro | ☐ | ☐ | |
| Registro de las licencias | ☐ | ☐ | |
| **CONFIGURACIÓN** | | | |
| **MODO DE OPERACIÓN SEGURO** | | | |
| Autenticación | ☐ | ☐ | |
| Sincronización Horaria | ☐ | ☐ | |
| Actualizaciones | ☐ | ☐ | |
| Auto-Chequeos | ☐ | ☐ | |
| Auditoría | ☐ | ☐ | |
| Backup | ☐ | ☐ | |
| **OPERACIÓN** | | | |
| **PROCEDIMIENTOS OPERATIVOS** | | | |

| ACCIONES | SÍ | NO | OBSERVACIONES |
|---|---|---|---|
| Comprobación periódica de fecha y hora del PC en el que está instalada la aplicación | ☐ | ☐ | |
| Definición y almacenamiento correcto de contraseña asociada a la clave privada | ☐ | ☐ | |
| Generación de par de claves pública-privada | ☐ | ☐ | |
| Borrado de clave no válidas | ☐ | ☐ | |
| Almacenamiento de claves revocadas | ☐ | ☐ | |
| Recepción de archivos cifrados con claves revocadas | ☐ | ☐ | |
| Descifrado de archivos cifrados con claves revocadas | ☐ | ☐ | |
| Definición/Comprobación de cripto periodos de claves públicas-privadas | ☐ | ☐ | |
| Distribución de las claves públicas | ☐ | ☐ | |
| La aplicación no debe estar desatendida una vez arrancada | ☐ | ☐ | |
| Cierre de la aplicación EP880 tras su uso | ☐ | ☐ | |
| Actualización de la aplicación | ☐ | ☐ | |
| Solicitud de nueva licencia | ☐ | ☐ | |
| Almacenamiento seguro del PC donde se instala el EP880 | ☐ | ☐ | |
| Actuaciones ante el comprometimiento del material cripto | ☐ | ☐ | |

## 5. REFERENCIAS

43. A continuación se indica la documentación del fabricante necesaria para la operación del *software* de cifrado EP880 y los documentos que han sido referenciados en este procedimiento:

**[REF.1]** Manual de usuario del EP880

Referencia: *EP270E880ZZ01*

## 6. ABREVIATURAS

| | |
|---|---|
| **AES** | *Advanced Encryption Standard* |
| **CPU** | *Central Processing Unit* |
| **CRC** | *Cyclic Redundancy Code* |
| **DRBG** | *Deterministic Random Bit Generator* |
| **ECCCDH** | *Elliptic Curve Cryptography Cofactor Diffie Hellman* |
| **ECKCDSA** | *Elliptic Curve Korean Certificate-based Digital Signature Algorithm* |
| **ENS** | Esquema Nacional de Seguridad |
| **GCM** | *Galois Counter Mode* |
| **HMAC** | *Hash Message Authentication Code* |
| **MAC** | *Media Access Control* |
| **RNG** | *Random Noise Generator* |
| **SHA** | *Secure Hash Algorithm* |
| **SW** | *Software* |

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL